



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 97195787.8

[45] 授权公告日 2003 年 9 月 24 日

[11] 授权公告号 CN 1122205C

[22] 申请日 1997.5.29 [21] 申请号 97195787.8

[30] 优先权

[32] 1996. 5. 31 [33] SE [31] 9602186 - 0

[86] 国际申请 PCT/SE97/00923 1997. 5. 29

[87] 国际公布 WO97/45780 英 1997. 12. 4

[85] 进入国家阶段日期 1998. 12. 23

[71] 专利权人 英普塞斯股份公司

地址 瑞典阿灵索斯

[72] 发明人 克里斯特·乔翰森 本特·托兰

审查员 谭 毅

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 杨国旭

权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称 防窃装置

[57] 摘要

本发明涉及一种用于计算机和其他辅助处理电子设备例如存储器部件、硬盘、插件板以及处理器的电子防窃装置。防窃装置包括一个与被保护部件集成在一起的阻塞电路，所述电路包括用于存储每个阻塞电路的特定身份代码的存储器。另外，电路还包括一个用于将密钥代码输入电路的输入端和一个用户将输入的密钥代码与电路的 ID 码相比较的比较器，电路适宜于在密钥码不正确的情况下中断部件的下一步使用。

1.用于计算机和其他辅助处理电子设备例如存储部件、硬盘、插件板以及处理器的电子防窃装置，其特征在于它包括一个与被保护部件集成在一起的阻塞电路，阻塞电路包括一个用于存储每个阻塞电路的特定身份代码（ID 码）的存储器，并且在于电路包括一个用于将密钥代码输入到电路中的通信终端和一个用于将输入的密钥代码与电路的 ID 码相比较的比较器，电路适合于在密钥代码不正确的情形中断部件的下一步使用。

2.根据权利要求 1 的电子防窃装置，其特征在于电路还包括一个时间延迟单元，在一个预设的时间周期期间延迟阻塞部件。

3.根据权利要求 1 或权利要求 2 的电子防窃装置，其特征在于被保护的部件是一个系统的一部分，该系统在存储器中包括一个用于包含在系统中并装备有防窃装置的不同部件的 ID 码寄存器，并且该系统在启动期间自动将密钥码送出到这些部件以控制这些部件，从而仅在系统和各部件的代码相符时系统才工作。

4.根据权利要求 1 或 2 的电子防窃装置，其特征在于 ID 码不是从电路可以得到的。

5. 根据权利要求 3 的电子防窃装置，其特征在于 ID 码不是从电路可以得到的。

6.根据权利要求 1 或 2 的电子防窃装置，其特征在于 ID 码永久存储在存储器中；

其特征还在于每一个防窃装置还包括阻塞电路中存储的唯一可以从外部利用的编号，从而能够建立一个包含有若干编号的数据寄存器，编号连结到用于最好包括防窃装置在内的所有部件的相应 ID 码，并且甚至可能将这个信息与关于例如部件主人的信息连结起来。

7. 根据权利要求 3 的电子防窃装置，其特征在于 ID 码永久存储在存储器中；

其特征还在于每一个防窃装置还包括阻塞电路中存储的唯一可以

从外部利用的编号，从而能够建立一个包含有若干编号的数据寄存器，编号连结到用于最好包括防窃装置在内的所有部件的相应 ID 码，并且甚至可能将这个信息与关于例如部件主人的信息连结起来。

防窃装置

5 本发明涉及一种用于例如说计算机和/或计算机部件例如存储器模块、插件板、硬盘等等的防窃装置。

在计算机行业中，特别是存储器模块、处理器、硬盘等等一类的计算机内部部件的窃贼数量近来显著上升，这对那些失窃者来说自然是个严重的问题。

10 由 EP - A2 - 687,968 已经知道在计算机中使用一种与计算机的启动联结的电路，它根据个人主权自动显示信息。身份数据存储在永久存储器中并在每次起动系统时检查身份。但是，该电路不防止非授权的个人直接使用计算机，也不防止计算机部件被偷。

15 为了补救这个问题，发明人提供一种使非授权使用所偷窃的计算机设备成为不能的系统。

因此，本发明的一个目的是提供一种防窃装置，它主要使非授权使用所偷窃的计算机或计算机部件变得更加困难。

20 本发明公开了一种用于计算机和其他辅助处理电子设备例如存储部件、硬盘、插件板以及处理器的电子防窃装置，其特征在于它包括一个与被保护部件集成在一起的阻塞电路，阻塞电路包括一个用于存储每个阻塞电路的特定身份代码（ID 码）的存储器，并且在于电路包括一个用于将密钥代码输入到电路中的通信终端和一个用于将输入的密钥代码与电路的 ID 码相比较的比较器，电路适合于在密钥代码不正确的情形中断部件的下一步使用。

25 为了举例说明的目的，下面将参照实施例和附图更详细地叙述本发明，其中：

图 1 示出本发明的基本构思；

图 2 一般地示出根据本发明的 ID 检验；

图 3 是检验电路的一个结构方框图；

图 4 是阻塞电路功能的一个流程图；以及

图 5 是根据一种应用的起动过程流程图。

正像图 1 中概略示出的，根据本发明的防窃装置涉及保护例如说计算机中的不同部件。在计算机起动时检验部件。这一点通过提供各自带有专门制造的识别电路（阻塞电路）的受保护部件、用识别电路检查进入部件的数据流达到。每个部件的各自阻塞电路都具有一个专用的身份代码（ID 码）。代码也输入主计算机并可在每次起动时自动检验，如图 2 所示。另一种办法是，代之以将代码存储在计算机硬盘等部件之中。万一计算机检出一个部件具有计算机不能接受的代码，系统便停止下来。而且连那个需要正确代码才工作的模块也被阻塞。这个电路的独特之处是它的单向通信，这意味着可以直接将信息输入电路而不能从电路中检索信息，从而保证了充分的安全性。

如果阻塞电路具有 64 位的工作性能，差不多可以得到 18.4×10^{18} 种可能的代码组合。此外，ID 码最好是永久存储。

由于这一安排，计算机之间无控制的模块（存储器、电路板等等）交换变为不可能。这意味着只有在计算机和各模块的代码相符时，计算机才能和它的各个模块一道工作。

阻塞电路的一个实施例示于图 3。这个电路包括两个 EEPROM 一类的永久存储器单元 301、302，一个存储器 301 用于存储 ID 代码，一个存储器 302 用于存储编号。编号可从电路的外面接收，而 ID 代码则不可。另外，电路还包括电源电压输入端 305 和一个数据输入端 304，以及一个用于将经由输入端 304 输入的数据与存储器 301 中存储的 ID 代码相比较的比较器。另外，电路包括一个输出端 306，利用它，电路能够阻塞电路位置所在的部件。这个输出端 306 以这样的方式连接到比较器，使得当经由输入端 304 输入的密钥码与所存储的 ID 码不符合时，电路便激活阻塞功能。

几个安装有阻塞电路的部件可以部分地具有同样的 ID 码，并因而可用同样的方法访问。这一点可通过所谓的掩蔽技术做到。根据掩蔽技术，仅有某些 ID 码子单元与密钥码相比较。这一点例如说对于那

些希望在公司计算机之间自由交换部件的商业企业是有利的。这种小组的可能数目随要被掩蔽的地点数目而定。

下面将参照图 4 的流程图更详细地叙述阻塞电路的功能。

1. 开始, 用电压 V_{cc} (例如 + 5VDC) 供应电路, 激活复位功能。
- 5 2. 在阻塞电路数据输入端 304 输入起动代码 (试起动代码), 然后, 电路准备接收一个控制字。
3. 然后输入控制字以控制电路。
4. 阻塞电路检验控制字是否准确, 如果不准确, 则阻塞电路截止, 将部件阻塞。
- 10 5. 控制字可以例如说包括将阻塞电路编号传送到电路的数据输出端。
6. 一个第二控制字可代之以包括一个掩蔽请求 (6a)。
7. 一个第三控制字提供差错寄存器的头前部分 (7a)。
8. 然后将系列号和型号输入到阻塞电路的数据输入端 304。
- 15 9. 然后将其余的数位 (55 - 0) 输入到阻塞电路的数据输入端 304。
10. 在存在有涉及掩蔽的控制字的情形, 阻塞电路比较包含有掩蔽的位图。当位图符合时 (10a), 阻塞电路将控制输出端设定到一个作用电平 (10b)。然后, 阻塞电路失去作用并在重新起动阻塞电路前, 输出端一直保持低电平。
- 20 11. 将差错寄存器减 1。
12. 如果差错寄存器达到 “0”, 则阻塞电路截止。
13. 否则, 阻塞电路恢复到接收新的密钥码的状态并回到第 8 条。
14. 停止阻塞电路的工作程序, 控制输出端仍留在以前的状态 (10b)。
- 25 下面, 将参照图 5 的流程图叙述具有被阻塞电路保护的部件的系统的起动过程。

1. 起动或使系统复位。
2. 系统接收器发生作用。
3. 系统进入阻塞电路控制程序。

4. 控制程序读出用于阻塞电路模块的设定系统参数。

5. 控制程序发出激活阻塞电路的试起动代码，将阻塞电路置于接收状态。

6. 控制程序将控制字发送到阻塞电路，控制字向阻塞电路发出关于
5 如何处理输入数据的指令。

7. 控制程序将掩蔽信息加上 (7a)，这是应当在设定时请求的。

8. 控制程序将头前数值加上 (8a)，这是应当在设定时请求的。

9. 第 7 条和/或第 8 条下面的任何信息都被传送到 (9a) 阻塞电路。

10. 控制程序读出用于 ID 码的设定信息。

10 11. 将信息传送到阻塞电路。

12. 将 ID 码传送到阻塞电路。

13. 控制程序检验增加的密钥码的到达。当需要掩蔽时，控制程序
不考虑这一点。在其他情况下读出一个新的 ID。

14. 控制程序完成并回到主程序。

15 15. 系统读出存储器中的参数并开始动作。

16. 系统进行自测试。

17. 自测试良好，则进行正常起动 (18)，否则显示出错误消息 (17a)。

18. 起动。

19. 系统锁定在环形回路中。

20 由于上面提到的差错寄存器，阻塞电路可以允许若干次错误的 ID
码输入尝试。允许这种尝试的次数随所指出的头前数值而定。每作一次
输入尝试，差错寄存器都减 1，并且当它达到 0 时，电路被阻塞以防止
接收另外的输入尝试。这个功能在 ID 码输入操作例如说由人工进行因
而可能发生手误等等的情形是所希望的。另外，在几个部件依次排列并
25 且所传送的数据必须到达所有的部件时也是所希望的。在这一情形，全
部的 ID 码都可以传送到所有的部件并且每个部件都认为别的部件的 ID
码是错误的尝试。

根据本发明的阻塞电路使得计算机之间或者计算机组之间的无控
制交换模块 (存储器、线路板、处理器等等) 成为不可能，因为计算机

和它的各个模块仅在计算机与模块代码相符合的条件下才能一道工作。这一点有效地减轻了电子防卫业务，也降低了特别是易于被偷商品的吸引力。

同样，可以设置不同阻塞电路的编号、ID 码以及所有权的数据寄存器。也可以把其他信息加给这种寄存器。但是，应当保护好这个寄存器，以确保只有警察当局和其他受权的个人或机构可以进行访问。寄存器可以被动方式使用以便于在偷盗等等情形下简化调查或者允许合法的主人找回所丢失的代码。也可以主动方式使用以供部件制造商、零售商等等在电路开始动作时根据特定的编号访问正确的 ID 码。

10 根据本发明的阻塞电路被集成在每个模块的电路图中并因其结构特点而将模块电路阻塞至使用正确的密钥为止。阻塞电路中的代码除了借助经由连接到阻塞电路的寄存器通过身份鉴别以外不能以任何方式从外部访问。另外，阻塞电路小到足以允许将它附装到任何的电子模块上。

15 最好，把阻塞电路也封装起来，使它完全不受外界的影响。

在制造设置有根据本发明的阻塞电路的计算机部件或电子部件的过程中，可在制造期间就已经将 ID 码存储在电路的存储器中。但是，这样做要求各个部件都附有适用于每个部件的 ID 代码清单，以允许代码在组装成系统时进入控制程序。

20 一种替代的方法是提供具有所谓暂停功能的防窃装置。这种延时功能意味着例如不激活闭锁电路，其结果是部件在一个一般为几分钟的预定时间周期上保持可接入访问。在这个时间周期期间，部件和阻塞电路可为用户服务，因而在组装成系统时，用户自己可以输入部件需要的 ID 码。但是，这些 ID 码仍然可以由部件制造商集中决定并在系统完成时
25 交给用户。

上面参照一个实施例叙述了本发明。但是，本发明可以有几个变例。例如，根据本发明的防窃装置可以用在除计算机以外的其他场合，例如借助某种处理器进行控制的移动电话、汽车和船舶内的电子组件等等。自然，也可以在 ID 部分、控制字等等之间使用具有不同组成部分的密

钥码，同样地，也可以使用不同长度的密钥码。再者，也可激活阻塞电路并以不同的方式例如通过无线电信号或其他的无线信号传输密钥码。在这种方式下，可以通过远程控制触发被偷器材如车辆、移动电话和类似设备中的阻塞电路。

- 5 实施例的这种修改应当认为是显然的并且正像所附权利要求书中界定的一样被包括在本发明的范围之内。

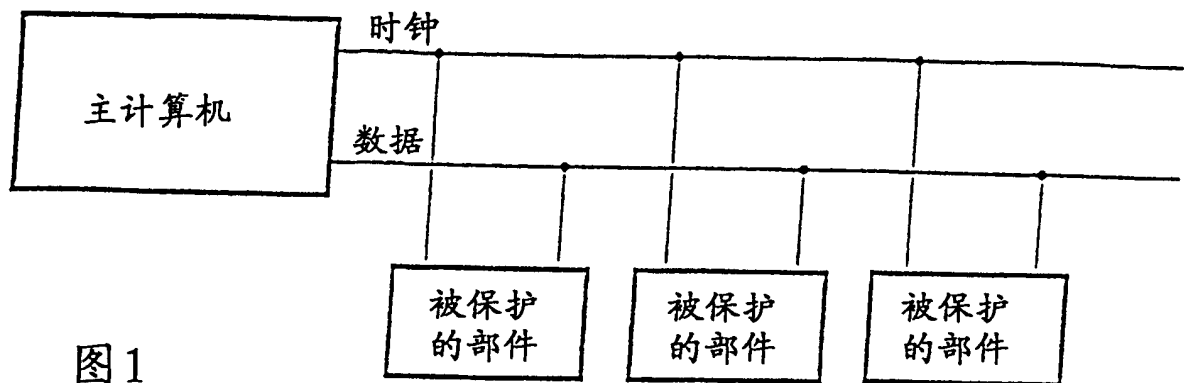


图 1

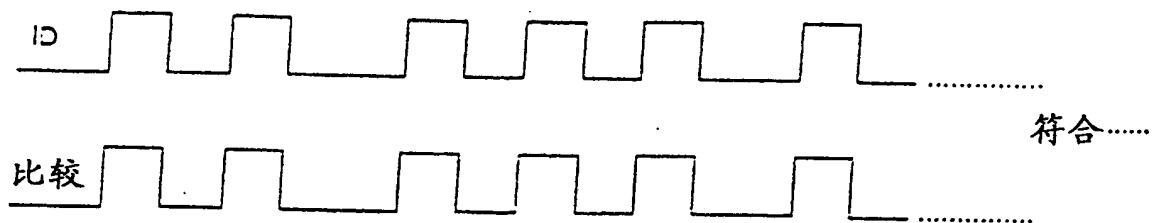


图 2

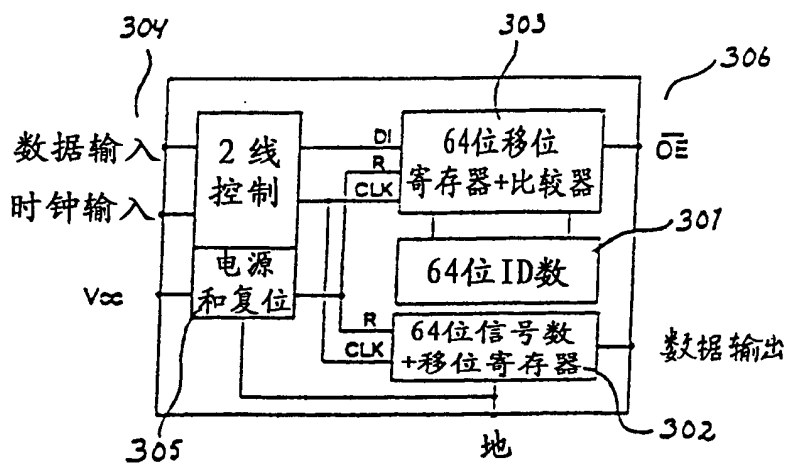


图 3

ID接收电路流程图

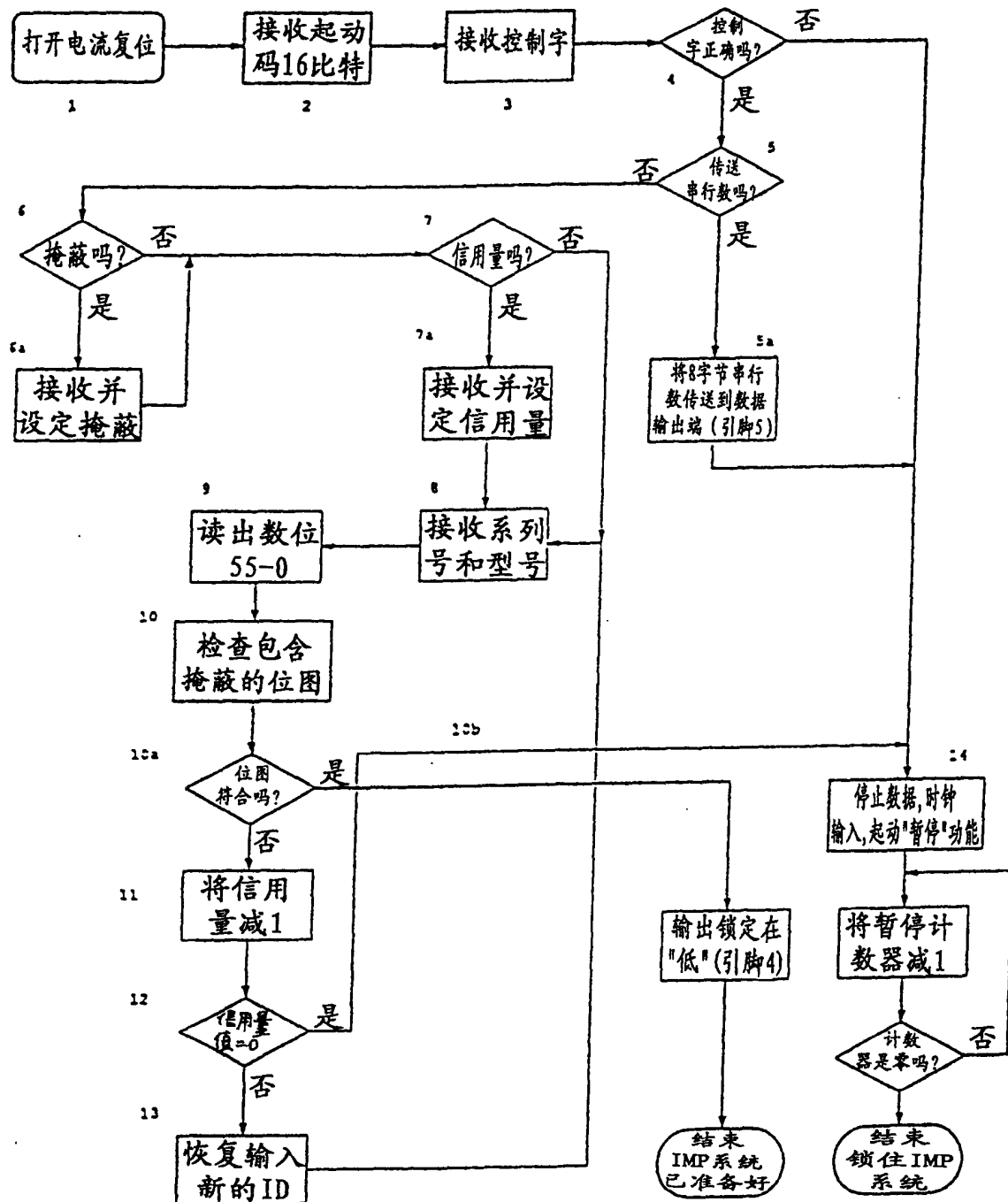


图 4

用于以 IMP 起动系统的流程图

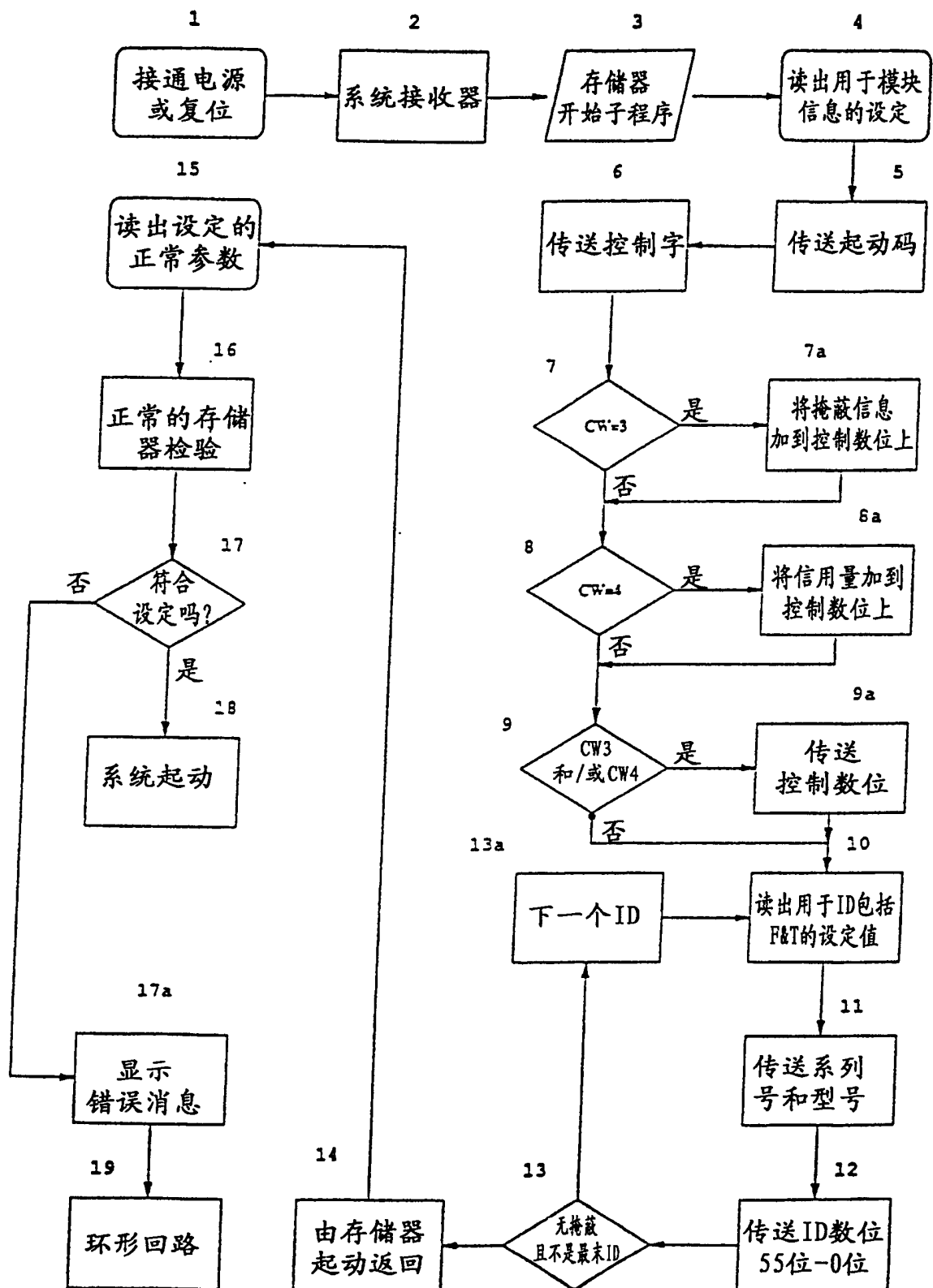


图 5